3. RINGS, IDEALS, AND GRÖBNER BASES

3.1. Polynomial rings and ideals

The main object of study in this section is a polynomial ring in a finite number of variables $R = k[x_1, \ldots, x_n]$, where $k$ is an arbitrary field.

The abstract concept of a ring $(R, +, \cdot)$ assumes that

1. operations $+$ (addition) and $\cdot$ (multiplication) are defined for pairs of ring elements,
2. both $(R, +)$ and $(R, \cdot)$ are abelian groups, i.e., both addition and multiplication are commutative,
3. multiplication distributes over addition: 
   $$(a + b)c = ac + bc, \quad a, b, c \in R,$$
4. there exist an additive identity, denoted by 0, and a multiplicative identity, denoted by 1, such that
   $$1 \cdot a = a,$$
5. there exists an additive inverse $-a$ for every $a \in R$:
   $$a + (-a) = 0.$$

The ring of polynomials possesses a natural addition and multiplication satisfying the above ring axioms. Moreover, it enjoys many other “nice” properties: for instance, the multiplication is cancellative:

$$fg = fh \implies g = h, \quad f, g, h \in R, \ f \neq 0,$$

which follows from the fact that a polynomial ring is an integral domain, i.e., a ring with no zero divisors: for $f, g \in R$,

$$fg = 0 \implies f = 0 \text{ or } g = 0.$$

Sometimes a polynomial ring $R = k[x_1, \ldots, x_n]$ is referred to as a polynomial algebra (over $k$) when one needs to emphasize that $R$ is a vector space over the field of coefficients $k$ equipped with a bilinear product; note that bilinearity here follows from the distributivity of multiplication in the definition of a ring.

**Note:** A field is a ring where each nonzero element has a multiplicative inverse.

In this text we mostly use fields such as $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ as coefficient fields in polynomial rings. However, one other field closely related to a polynomial ring $R = k[x_1, \ldots, x_n]$ is the field of rational functions, denoted by $k(x_1, \ldots, x_n)$, the elements of which are of the form

$$\frac{f}{g}, \quad \text{where } f, g \in R; \quad \left(\frac{f}{g} = \frac{f'}{g'} \iff fg' = f'g\right).$$

Every nonzero element $f/g$ has $(f/g)^{-1} = g/f$ as its multiplicative inverse.

**3.1.1. Ideals.** An ideal of $R$ is a nonempty $k$-subspace $I \subseteq R$ closed under multiplication by elements of $R$:

$$gI = \{gf \mid f \in I\} \subseteq I, \quad g \in R.$$

Two trivial ideals of $I$ are the zero ideal $\{0\}$ (denoted by $0$) and the whole ring $R$. One way to construct an ideal is to generate one using a finite set of polynomials.

For $f_1, \ldots, f_r \in R$, we define

$$\langle f_1, \ldots, f_r \rangle = \{g_1f_1 + \cdots + g_rf_r \mid g_i \in R\} \subseteq R,$$
the set of all linear combinations of generators \( f_i \) with polynomial coefficients \( g_i \). The fact that the set \( I = \langle f_1, \ldots, f_r \rangle \) is an ideal follows straightforwardly from the definition.

The set \( I = \langle f \rangle = \{ gf \mid g \in R \} \) for an element \( f \in R \) is called a principal ideal and \( f \) is called a principal generator of \( I \). Note that \( R = \langle 1 \rangle \).

**Exercise 3.1.1.** A ring, each ideal of which is principal, is called a principal ideal domain (PID). Show that the ring of univariate polynomials is a PID.

We can construct an ideal using an arbitrary (possibly infinite) set of generators \( G \subseteq R \):

\[
\langle G \rangle = \bigcup_{F \subseteq G, |F| < \infty} \langle F \rangle.
\]

However, every ideal \( I \subseteq R \) is finitely generated, i.e., \( I = \langle f_1, \ldots, f_r \rangle \) for some finite number \( r \) of polynomials \( f_i \in R \) (see Theorem 3.2.10). This is yet another “nice” property of \( R \): a ring with such property is called Noetherian.

**Exercise 3.1.2.** A ring is said to satisfy the ascending chain condition (ACC) if every chain of ideals

\[
I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots
\]

stabilizes, i.e., there is \( i_0 \) such that \( I_i = I_{i_0} \) for all \( i > i_0 \).

For an arbitrary ring, show that this condition is equivalent to the condition of all ideals being finitely generated.

**Example 3.1.3.** Consider an ideal \( I = \langle x + y, x^2 \rangle \subseteq k[x, y] \). However, we can pick another set of generators of \( I \); for instance, \( I = \langle x + y, y^2 \rangle \).

The polynomials in the second set of generators belong to \( I \) as \( y^2 = (x^2) + (y - x)(x + y) \).

This shows the containment \( \langle y^2, x + y \rangle \subseteq I \). Since, in a similar way, the reverse containment can be shown, the ideals are equal.

**Exercise 3.1.4.** Determine whether the following subsets of \( R \) are ideals:

1. \( k \), the field of coefficients;
2. a subring \( k[x_1, \ldots, x_m] \subset R = k[x_1, \ldots, x_n] \), where \( 0 < m < n \);
3. polynomials with no constant term;
4. \( R_{\leq d} \), polynomials of degree at most \( d \);
5. homogeneous polynomials, i.e., polynomials with all terms of the same degree.

**3.1.2. Sum, product, and intersection of ideals.** The sum of two ideals \( I \) and \( J \) (as \( k \)-subspaces),

\[
I + J = \{ f + g \mid f \in I, g \in J \},
\]

is an ideal. So is the intersection

\[
I \cap J = \{ f \mid f \in I, f \in J \}.
\]

**Exercise 3.1.5.** Prove that \( I + J \) is the smallest ideal containing \( I \) and \( J \). Show that, if \( I = \langle f_1, \ldots, f_r \rangle \) and \( J = \langle g_1, \ldots, g_s \rangle \), then \( I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle \).
Exercise 3.1.6. Show that the ideal generated by products of elements in $I$ and $J$,
\[ IJ = \langle fg \mid f \in I, g \in J \rangle, \]
is contained in $I \cap J$. (Exercise 3.1.7 shows that $IJ \neq I \cap J$ in general.)

Exercise 3.1.7. Consider the univariate polynomial ring $R = k[x]$.

1. How would one find a principal generator of $\langle f \rangle \cap \langle g \rangle$?
2. How would one find a principal generator of $\langle f \rangle \langle g \rangle$?
3. Give an example of $f$ and $g$ where the ideals above (the intersection and the product) are not the same.

3.1.3. Ring maps and quotient rings. Let $R$ and $S$ be rings, a map $R \to S$ is called a ring map if it respects both additive and multiplicative structure of the rings.

Example 3.1.8. The following ring maps involving polynomial rings are frequently used:

- specialization of a variable
  \[ (\cdot)|_{x_i=a_i} : k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_i=a_i, x_{i+1}, \ldots, x_n], \quad a_i \in k, \]
  \[ f = f(x_1, \ldots, x_n) \mapsto f|_{x_i=a} = f(x_1, \ldots, x_{i-1}, a_i, x_{i+1}, \ldots, x_n); \]

- evaluation at a point $a = (a_1, \ldots, a_n) \in k^n$,
  \[ e_a : k[x_1, \ldots, x_n] \to k, \]
  \[ f(x_1, \ldots, x_n) \mapsto f(a_1, \ldots, a_n); \]

- variable substitution:
  \[ k[x_1, \ldots, x_n] \to k[y_1, \ldots, y_m], \]
  \[ f(x_1, \ldots, x_n) \mapsto f(g_1(y_1, \ldots, y_m), \ldots, g_n(y_1, \ldots, y_m)), \]
  where $g_1, \ldots, g_n$ are polynomials in the ring $k[y_1, \ldots, y_m]$.

Every polynomial ring map can be defined as the last map in Example 3.1.8, since every ring map is determined by its action on the ring generators of the domain, which in case of a polynomial ring are the variables.

A map $\phi : R \to S$ is called an isomorphism, if there is a map $\psi : S \to R$ (called the inverse map of $\phi$) such

\[ \psi \phi = \text{id}_R \text{ and } \phi \psi = \text{id}_S, \]

where $\text{id}_R : R \to R$ denotes the identity map on $R$.

Exercise 3.1.9. Let $R = k[x_1, \ldots, x_n]$. A matrix $A \in k^{(n+1) \times n}$ defines a linear substitution

\[ \begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix} = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in R^n \]

that can be used to make an endomorphism (the source and target of the map coincide) $\phi_A : R \to R$ using the recipe of last map in Example 3.1.8. If the ring map $\phi_A$ is an automorphism (endomorphism that is an isomorphism), it is commonly referred to as a linear change of coordinates.
(1) Find a condition on $A$ for $\phi_A$ to be an automorphism (endomorphism that is an isomorphism).

(2) If $\phi_A$ is an automorphism, find $B$ such that $\phi_B$ is its inverse.

**Exercise 3.1.10.** Prove that the kernel of a polynomial ring map, i.e., the set of elements that map to zero, is an ideal.

Given an ideal $I \subseteq R$ we introduce the **quotient ring** $R/I$. The elements of $R/I$ are equivalence classes $[f] = \{ g \in R \mid f - g \in I \} \subseteq R$ where $f \in R$. Two elements $f, g \in R$ are equivalent *modulo* $I$ if $[f] = [g]$; that, in turn, holds iff $f - g \in I$.

The ring structure of $R/I$ is induced by that of the ring $R$:

- $[f] + [g] = [f + g]$;
- $[f][g] = [fg]$;
- $[0]$ is the additive and $[1]$ is the multiplicative identities.

The addition above is well defined: if $f' \in [f], g' \in [g]$ are alternative representatives then $[f' + g'] = [f + g]$, since $f' + g' - (f + g) = (f' - f) + (g' - g) \in I$.

**Exercise 3.1.11.** Show that the product in a quotient ring is well defined.

There is a natural surjective ring map $\phi : R \to R/I$

$$ f \mapsto [f] $$

**Proposition 3.1.12.** Let $I$ be an ideal in an arbitrary ring $R$. There is a one-to-one correspondence between ideals of $R/I$ and ideals of $R$ containing $I$. Sums, intersections, and products of ideals are preserved under this correspondence.

**Proof.** We claim that the ring map $\phi$ above establishes a one-to-one correspondence.

Take an ideal $J \subseteq R$, then $\phi(J)$ is an ideal of $J$; in fact, this is true for any map $\phi$. This follows from the definition of an ideal and the fact that $\phi$ respects the ring addition and multiplication. Similarly, if $J$ is an ideal of $R/I$ then $\phi^{-1}(J)$ is an ideal of $R$; it contains the preimage of zero $\phi^{-1}([0]) = I$. □

**Exercise 3.1.13.** Let $R = k[x_1, \ldots, x_n]$ and $I = \langle x_{m+1}, \ldots, x_n \rangle$. Show that the rings $R/I$ and $S = k[x_1, \ldots, x_m]$ are isomorphic via a natural ring map $\psi : R/I \to S$,

$$ \psi([f]) = f(x_1, \ldots, x_m, 0, \ldots, 0) \in S, \quad f \in R. $$

**Exercise 3.1.14.** Consider ideal $I = \langle x^2 + 1 \rangle \subseteq \mathbb{Q}[x]$. Prove that the quotient ring $\mathbb{Q}[x]/I$ is a field; it is called the field of Gaussian rational numbers. (Hint: For each element of $\mathbb{Q}[x]/I$ find a “small” representative in $\mathbb{Q}[x]$ and then determine its inverse.)
3.2. Gröbner bases

It has been pointed out (e.g., in Example 3.1.3) that the same nonzero ideal can be generated by different sets of generators. In this section we develop a theory and algorithms to convert any generating sets into a Gröbner basis, a generating set with helpful special properties.

3.2.1. Monomial orders. A monomial order is a recipe for comparing two monomials in a polynomial ring \( R = k[x_1, \ldots, x_n] \) with the following properties:

(1) It is a total order: for every pair of distinct monomials \( x^\alpha \) and \( x^\beta \), \( \alpha, \beta \in \mathbb{N}^n \), either \( x^\alpha > x^\beta \) or \( x^\alpha < x^\beta \).

(2) It is a multiplicative order: \( x^\alpha > x^\beta \Rightarrow x^\alpha \gamma > x^\beta \gamma \), \( \alpha, \beta, \gamma \in \mathbb{N}^n \).

(3) It is a well-order: every nonempty set (of monomials) has a minimal element. Together with being a total order, this implies that \( x^0 = 1 < x^\alpha \), \( \alpha \in \mathbb{N}^n - \{0\} \).

Exercise 3.2.1. Show that there is only one monomial order for monomials of a univariate polynomial ring.

Example 3.2.2. A lexicographic order on \( k[a, b, c, \ldots, z] \) compares monomials as words in a dictionary: \( a^3b^2c = aaabc > aabbcccc = a^2b^3c^4 \) as “aaabc” comes before “aabbcccc” in the dictionary.

This can be used with any alphabet: for \( k[x_1, \ldots, x_n] \), we have \( x^\alpha >_\text{lex} x^\beta \iff \alpha_1 > \beta_1 \) or (\( \alpha_1 = \beta_1 \) and \( x^{(0, \alpha_2, \ldots, \alpha_n)} >_\text{lex} x^{(0, \beta_2, \ldots, \beta_n)} \)).

One important class of monomial orders is graded monomial orders, the ones that refine the (non-total) order by degree.

Example 3.2.3. The graded lexicographic order compares the degrees of monomials first and “breaks the tie”, if necessary, using the lexicographic order: \( x^\alpha >_\text{glex} x^\beta \iff |\alpha| > |\beta| \) or (\( |\alpha| = |\beta| \) and \( x^\alpha >_\text{lex} x^\beta \)).

Note: The default monomial order used by many computer algebra systems is graded reverse lexicographic order.

Exercise 3.2.4. For a polynomial \( f = x^3y + 2x^2y^2 + xy^3 + x + y^2 + y + 1 \) find \( \text{LM}(F) \), where

- (1) \( \gg >_\text{lex}, x > y \);
- (2) \( \gg >_\text{lex}, y > x \);
- (3) \( \gg >_\text{glex}, x > y \);
- (4) \( \gg >_\text{glex}, y > x \).

Another useful class of monomial orders are block orders that compare monomials according to a fixed partition of the sets of variables into blocks.
Let \( > \) be an order on the monomials in \( x_1, \ldots, x_m \) and \( >_2 \) be another order on monomials in \( x_{m+1}, \ldots, x_n \). The 2-block order \( >_{2,1} \) on monomials in \( x_1, \ldots, x_n \) is defined as:

\[
x^{\alpha_1} >_{1,2} x^{\beta} \iff x_{m+1}^{\alpha_{m+1}} \cdots x_n^{\alpha_n} >_2 x_{m+1}^{\beta_{m+1}} \cdots x_n^{\beta_n}
\]

or

\[
(x_{m+1}^{\alpha_{m+1}} \cdots x_n^{\alpha_n} = x_{m+1}^{\beta_{m+1}} \cdots x_n^{\beta_n} \text{ and } x_1^{\alpha_1} \cdots x_m^{\alpha_m} >_1 x_1^{\beta_1} \cdots x_m^{\beta_m}).
\]

Note that \( >_{\text{lex}} \) is a 2-block order with respect to the blocks \( \{x_1, \ldots, x_m\} \) and \( \{x_{m+1}, \ldots, x_n\} \).

### 3.2.2. Normal form algorithm.

In §1.1.4 we have introduced \( \text{NF}_f \) the normal form function that maps a polynomial \( g \in k[x] \) to its remainder after division by the polynomial \( f \in k[x] \). We would like to define the normal form \( \text{NF}_F: R \to R \), where \( R = k[x_1, \ldots, x_n] \), with respect to a system of polynomials \( F \in R^r \).

**Algorithm 3.2.1**

\[
h = \text{NF}(g, F)
\]

**Require:** \( g \in R; \) \( F \in R^r, r > 0; \)

**Ensure:** \( h \in R, \) such that

\[
(3.2.1) \quad g = h + \sum_{i=1}^{r} q_i f_i, \quad q_i \in R, \text{ deg } q_i + \text{ deg } f_i \leq \text{ deg } g
\]

and either \( h = 0 \) or \( \text{LM}(h) \) is not divisible by \( \text{LM}(f) \) for all \( f \in F \).

\[
h \leftarrow g
\]

**while** \( h \neq 0 \) and \( \text{LM}(h) \) is divisible by \( \text{LM}(f) \) for some \( f \in F \) do

\[
f \leftarrow \text{first polynomial in the set } F \text{ such that } \text{LM}(f) | \text{LM}(h)
\]

\[
\begin{align*}
&h \leftarrow h - \frac{\text{LT}(h)}{\text{LT}(f)} f \\
&\text{end while}
\]

The leading monomials and leading terms in Algorithm 3.2.1 are taken with respect to a fixed monomial order \( > \). If this needs to be emphasized, we write \( \text{NF}_F^{(>)} \); normal forms for the same input, but different monomial orders are not the same, in general.

**Proof of termination and correctness of Algorithm 3.2.1.** Let \( h_i \) be the contents of \( h \) at the \( i \)-th iteration. Then

\[
\text{LM}(h_1) > \text{LM}(h_2) > \text{LM}(h_3) > \cdots
\]

Since a monomial order is a well-order, the descending sequence of monomials terminates, so does the algorithm. The condition (3.2.1) holds for all \( h = h_i \) by construction. When the algorithm terminates \( h \) is either 0 or \( \text{LM}(h) \) is not divisible by \( \text{LM}(f) \) for all \( f \in F \).

**Exercise 3.2.5.** Let \( f_1, \ldots, f_r \in I \), where \( I \subseteq R \) is an ideal.

Show that \( \text{NF}_{(f_1, \ldots, f_r)}(g) \in I \) iff \( g \in I \).

**Note:** As its univariate analogue, Algorithm 3.2.1 can be modified to compute not only the “remainder”, but also the “quotients”, i.e., polynomial coefficients \( q_i \in R \) in (3.2.1).

Note that, in general, the normal form also depends on the order of polynomials in the system.
Example 3.2.6. Consider two polynomials in $k[x, y, z]$,

\[
\begin{align*}
  f_1 &= x - y, \\
  f_2 &= x - z^2.
\end{align*}
\]

Fix the monomial order $\succ \succ_{\text{lex}} x > y > z$.

Then $\text{NF}(f_1, f_2)(x) = y$ and $\text{NF}(f_2, f_1)(x) = z^2$.

Exercise 3.2.7. For $f_1 = x^3 + y^2$, $f_2 = xy + 1$, and

\[
g = x^3y + 2x^2y^2 + xy^3 + x + y^2 + y + 1,
\]

polynomials in $k[x, y]$ with the lexicographic order such that $x > y$, find

1. $\text{NF}(f_1, f_2)(g)$
2. $\text{NF}(f_2, f_1)(g)$

3.2.3. Initial ideal, Dickson’s Lemma, Noetherianity. For a polynomial ideal $I \subset R$, the ideal generated by the leading monomials of all polynomials of $I$ is called the initial ideal and denoted

\[
in(I) = \langle \text{LM}(f) \mid f \in I \rangle.
\]

Again, if we need to emphasize the (usually fixed) monomial order $> >$ that is used, we would write $\text{in}_{> >}(I)$.

Exercise 3.2.8. For the ideal $I = \langle x - y, x - z^2 \rangle \subset k[x, y, z]$ find

1. the initial ideal $\text{in}_{\text{lex}}(I)$ with respect to the lexicographic ordering;
2. the initial ideal $\text{in}_{g \text{lex}}(I)$ with respect to the graded lexicographic ordering.

We need the following lemma to show that every ideal $I$ of a polynomial ring $R$ can be finitely generated; this is one of the ways to say that $R$ is Noetherian.

(We refered to this fact in §3.1.1 without a proof.)

Lemma 3.2.9 (Dickson’s Lemma). Every monomial ideal (i.e., ideal generated by monomials) is finitely generated.

Theorem 3.2.10. A polynomial ring $R$ is Noetherian.

Proof. Let $I \subseteq R$ be a nonzero ideal of $R$, then, by Dickson’s Lemma, its initial ideal is finitely generated:

\[
\text{in}(I) = \langle m_1, \ldots, m_r \rangle, \quad r > 0.
\]

Pick $f_i \in I$ such that $\text{LM}(f_i) = m_i$ and let

\[
J = \langle f_1, \ldots, f_r \rangle, \quad J \subseteq I.
\]

Take $g \in I$ and compute $h = \text{NF}(f_1, \ldots, f_r)(g)$. On one hand, by Exercise 3.2.5, $h \in I$. On the other, if $h \neq 0$, then $\text{LM}(h) \notin \text{in}(I)$ as it is not divisible by monomials $m_i$, which leads to a contradiction. Therefore, $h = 0$ and $g \in J$; we conclude that $J = I$. 

Proof of Dickson’s Lemma. Let $G$ be a (possibly infinite) set monomials generating the ideal $J = \langle G \rangle$. Without a loss of generality we may assume $G$ consists of minimal elements with respect to divisibility: if two monomials $x^\alpha, x^\beta \in G$ are such that $x^\alpha$ divides $x^\beta$, then the latter can be excluded from $G$.

First, we can see a monomial ideal $J \subseteq k[x_1, \ldots, x_n]$ generated as follows

\[
J = \langle J_0 \cup x_1J_1 \cup x_1^2J_2 \cup \cdots \rangle,
\]
where \( J_i \subseteq k[x_2, \ldots, x_n] \) are monomial ideals (in a ring with one fewer variable) such that
\[
\{ x_{1}^{i}x_{2}^{\beta_{2}} \cdots x_{n}^{\beta_{n}} \mid x_{2}^{\beta_{2}} \cdots x_{n}^{\beta_{n}} \in \text{in}(J_i) \} = \{ x_{1}^{\alpha_{1}}x_{2}^{\alpha_{2}} \cdots x_{n}^{\alpha_{n}} \mid \alpha_{1} = i \}.
\]

Using induction on the number of variables in a polynomial ring, we may assume that \( k[x_2, \ldots, x_n] \) is Noetherian. The base of induction is the case \( R = k \), a polynomial ring with no variables, which has only trivial ideals.

Observe that \( J_1 \subseteq J_2 \subseteq \cdots \) is an ascending chain of ideals. By Noetherianity it stabilizes; we also may pick finite generating sets of monomials \( G_i \) for \( J_i \).

Now the infinite union above becomes finite: for some \( s > 0 \),
\[
J = \langle J_0 \cup x_1 J_1 \cup x_1^2 J_2 \cup \cdots \cup x_1^s J_s \rangle
= \langle J_0 \cup x_1 G_1 \cup x_1^2 G_2 \cup \cdots \cup x_1^s G_s \rangle,
\]
which shows that \( J \) is generated by a finite number of monomials. \( \square \)

### 3.2.4. Gröbner bases and their properties

Fix a polynomial ring \( R \) and a monomial order.

A set \( G \subseteq R \) is a Gröbner basis of an ideal \( I \subseteq R \) if
- \( I = \langle G \rangle \), and
- \( \text{in}(I) = \langle \text{in}(G) \rangle \), where \( \text{in}(G) = \{ \text{in}(g) \mid g \in G \} \).

**Example 3.2.11.** The set \( G = \{ x - y, x - z^2 \} \subseteq k[x, y, z] \) is
- not a Gröbner basis of \( I = \langle G \rangle \) with respect to \( >_{\text{lex}(x,y,z)} \), since \( \text{in}(I) \ni y = \text{in}(y - z^2) \), however \( \text{in}(G) = \langle x \rangle \nmid y \);
- a Gröbner basis of \( I = \langle G \rangle \) with respect to \( >_{\text{lex}(z,y,x)} \); one can show that \( \text{in}_{\text{lex}(z,y,x)}(I) = \langle y, z^2 \rangle \).

**Proposition 3.2.12.** Let \( G \) be a Gröbner basis of an ideal \( I \) and consider a polynomial \( f \in R \).

1. \( \text{NF}_G(f) = 0 \iff f \in I. \)

**Proof.** Let \( h = \text{NF}_G(f) \); note that \( h \in I \iff f \in I \), by Exercise 3.2.5. However, either \( h = 0 \) or \( \text{LM}(h) \notin \text{in}(I) \), since the leading monomials of elements in \( G \) generate \( \text{in}(I) \). The conclusion is that \( h \in I \iff h = 0. \) \( \square \)

Given a fixed monomial order, define the **normal form** \( \text{NF}_I(f) \) of \( f \in \mathcal{R} \) with respect to an ideal \( I \) to be the output of Algorithm 3.2.2.

**Corollary 3.2.13** (of Proposition 3.2.12). A polynomial \( f \in R \) belongs to an ideal \( I \subseteq R \) iff \( \text{NF}_I(f) = 0. \)

**Proposition 3.2.14.** There is a unique \( h \in R \), such that \( h \equiv f \pmod{I} \) and all monomials of \( h \) are not in \( \text{in}(I) \).

**Proof.** Suppose two distinct \( h', h \in R \) satisfy the hypotheses. On one hand, \( h - h' = (h - f) - (h' - f) \in I \); on the other, monomials of \( h - h' \) do not belong to \( \text{in}(I) \), hence, \( h - h' = \text{NF}_I(h - h') \). We conclude that \( h - h' = 0 \) by Corollary 3.2.13. \( \square \)

**Corollary 3.2.15.** For any polynomial \( f \in R \) and any ideal \( I \subseteq R \), the normal form \( \text{NF}_I(f) \) does not depend
- neither on the choice of the Gröbner basis \( G \) in Algorithm 3.2.2
- nor on the order of reductions in Algorithm 3.2.1.
Algorithm 3.2.2 $h = \text{NF}(f, I)$

Require: $f \in R = k[x_1, \ldots, x_n]$ with a fixed monomial order; $I \subseteq R$, an ideal (given by a finite set of generators);

Ensure: $h \in R$, such that $h \equiv f \pmod{I}$ and all monomials of $h$ are not in $\text{in}(I)$.

$G \leftarrow$ a Gröbner basis of $I$
$h \leftarrow 0$
$t \leftarrow f$ \quad -- This is the “tail” that we reduce.

while $t \neq 0$ and $\text{LM}(t)$ is divisible by $\text{LM}(g)$ for some $g \in G$ do
    $t \leftarrow \text{NF}_G(t)$
    if $h \neq 0$ then
        $h \leftarrow h + \text{LT}(t)$
        $t \leftarrow t - \text{LT}(t)$
    end if
end while

A Gröbner basis $G$ of an ideal $I$ is called reduced if
- $\text{LC}(g) = 1$ for all $g \in G$ (g is monic),
- $\text{LM}(g)$, $g \in G$, are distinct,
- $\text{NF}_I(g - \text{LM}(g)) = g - \text{LM}(g)$ (no other monomials in $\text{in}(I)$).

Exercise 3.2.16. Show that (provided a fixed monomial order) the reduced Gröbner basis is unique for any ideal.

Exercise 3.2.17. Fix the monomial order $>_\text{glex}$. Knowing that

$$G = \{2x^2 - 2y^2, \ y^3 - xy^2 + xy - x^2, \ xy^2 - 3xy + 2x\}$$

is a Gröbner basis of the ideal $I = \langle G \rangle$, find the reduced Gröbner basis of $I$.

3.2.5. Buchberger’s algorithm. Now we are ready to provide the missing piece of Algorithm 3.2.2 is a subroutine that would compute a Gröbner basis for an ideal generated by a finite set of polynomials.

For two nonzero polynomials $f, g \in R$. Define the $s$-polynomial of $f$ and $g$

$$S_{f,g} = \frac{\text{LT}(g)}{\gcd(\text{LM}(f), \text{LM}(g))} f - \frac{\text{LT}(f)}{\gcd(\text{LM}(f), \text{LM}(g))} g \in R.$$  

Theorem 3.2.18 (Buchberger’s criterion). Let $G \subseteq R$ be a finite set of polynomials, then $G$ is a Gröbner basis of the ideal $I = \langle G \rangle$ (with respect to a fixed monomial order) iff $\text{NF}_G(S_{f,g}) = 0$ for all $f, g \in G$.

Proof. If $G$ is a Gröbner basis, then $S_{f,g} \in I$ implies $\text{NF}_G(S_{f,g}) = 0$ by Proposition 3.2.12. To prove the statement in the other direction, we will show that, when every $s$-polynomial reduces to zero, every element $f \in I$ also reduces to zero with respect to $G$. This is sufficient, since it implies $\text{in}(I) = \langle \text{in}(G) \rangle$.

Let $G = \{g_1, \ldots, g_r\}$. If $f = \sum_{i=1}^r h_ig_i$ for $h_i \in R$, we shall call the sequence $h = (h_1, \ldots, h_r)$ a representation of $f \in I$. Define the leading monomial $\lambda$ of a representation to be

$$\lambda = \lambda(h) = \max_{i} \text{LM}(h_ig_i)$$

and the multiplicity $\mu$ of the representation to be the number of times the equality $\text{LM}(h_ig_i) = \lambda(h_1, \ldots, h_r)$ holds for $i = 1, \ldots, r$.  

Let $f = \text{NF}_G(f)$ be a (reduced) polynomial in $I$ and suppose it is nonzero. Suppose $(h_1, \ldots, h_r)$ is a representation of $f$ with the smallest possible leading monomial $\lambda$ and multiplicity $\mu$.

If $\mu = 1$, then $\text{LM}(f) = \text{LM}(h_i g_i)$ for some $i$, which contradicts our assumption (that $f$ is reduced).

For $\mu > 1$, take $1 \leq i < j \leq r$ such that $\text{LM}(h_i g_i) = \text{LM}(h_j g_j)$. This means that for the monomial $m = \lambda / \text{lcm}(\text{LM}(g_i), \text{LM}(g_j))$ and some $c \in k$,

$$\text{LT}(h_i) g_i = c m \text{lcm}(\text{LM}(g_i), \text{LM}(g_j)).$$

Since $\text{NF}_G(S g_i, g_j) = 0$, there are $\hat{h}_i$ such that

$$S g_i, g_j = \sum_{i=1}^r \hat{h}_i g_i \quad \text{and} \quad \text{LM}(\hat{h}_i g_i) < \text{lcm}(\text{LM}(g_i), \text{LM}(g_j)).$$

One can check that representation $h'$ of $f$ (obtained by adding a representation of 0 corresponding to the above),

- $h'_l = h_l + c m \hat{h}_l$, if $l \notin \{i, j\}$;
- $h'_i = h_i - c m \left( \frac{\text{LT}(g_j)}{\text{gcd}(\text{LM}(g_i), \text{LM}(g_j))} + \hat{h}_i \right)$;
- $h'_j = h_j + c m \left( \frac{\text{LT}(g_i)}{\text{gcd}(\text{LM}(g_i), \text{LM}(g_j))} + \hat{h}_j \right)$,

has either $\lambda(h') < \lambda(h)$ (this happens if $\mu(h) = 2$) or $\lambda(h') = \lambda(h)$ but $\mu(h') < \mu(h)$. This contradicts the minimality of representation $h$. Hence, $\text{NF}_G(f) = 0$ for every $f \in I$. \qed

The criterion translates into Buchberger's algorithm for finding a Gröbner basis (Algorithm 3.2.3).

**Algorithm 3.2.3** $G = \text{Buchberger}(I)$

**Require:** $I = \langle F \rangle \subseteq R$, an ideal given by a finite set of generators $F$;

**Ensure:** $G \subseteq R$, a Gröbner basis of $I$ (with respect to a fixed monomial order).

\[
\begin{align*}
G & \leftarrow F \\
S & \leftarrow G \times G \\
\text{while} \ S \neq \emptyset \ \text{do} \\
& \quad \text{Pick} \ (f_1, f_2) \in S. \\
& \quad S \leftarrow S - \{(f_1, f_2)\} \\
& \quad g \leftarrow \text{NF}_G(S f_1, f_2) \\
& \quad \text{if} \ g \neq 0 \ \text{then} \\
& \quad \quad S \leftarrow S \cup \{g\} \times G \\
& \quad \quad G \leftarrow G \cup \{g\} \\
& \quad \text{end if} \\
\text{end while}
\end{align*}
\]

**Proof of termination and correctness of Algorithm 3.2.3.** Let $G_i$ be an intermediate set of generators at step $i$ of the algorithm. The sequence

$$G_1 \subseteq G_2 \subseteq \cdots$$
has a property that either $G_{i+1} = G_i$ or $\text{LM}(G_i) \subseteq \text{LM}(G_{i+1})$, which which mirrors in the sequence
\[
\langle \text{LM}(G_1) \rangle \subseteq \langle \text{LM}(G_2) \rangle \subseteq \cdots
\]
Since the latter sequence has to stabilize due to Noetherianity of the polynomial ring, the former one stabilizes too. This means that no new elements are appended to the set $G = G_{final}$ after some step and the algorithm runs through the remaining s-pairs reducing each of them to zero and stops.

The s-polynomials of s-pairs that resulted in a new element $g \in G$ reduce to zero, since $g \in G_{final}$. Therefore, every s-pair considered during the run reduces to zero and the algorithm goes through all pairs $G_{final} \times G_{final}$ by construction. □
3.3. Basic computations in polynomial rings

Here we discuss basic computations in polynomial rings that Gröbner bases enable.

Proposition 3.2.12 already provides us with a way to test if a polynomial belongs to an ideal: the so-called ideal membership test.

3.3.1. Computations in a quotient ring. Given an ideal \( I \subseteq R \) consider the quotient ring \( R/I \). Proposition 3.2.14 and Corollary 3.2.15 give a way to pick a canonical representative for \( f \in R/I \): take the normal form of the representative \( f \in R \):
\[
[\text{NF}_I(R)] = [f].
\]
Note that representation with normal forms gives a one-to-one correspondence between polynomials involving only standard monomials (i.e., monomials outside \( \text{in}(I) \)) and \( R/I \).

Example 3.3.1. The set
\[
G = \left\{x^2 - y^2, \left(y^3\right) - 2xy - y^2 + 2x, \left(xy^2\right) - 3xy + 2x\right\}
\]
is a Gröbner basis of \( I = (G) \) with respect to \( \text{glex} \). The \( S = \{1, x, xy, y^2\} \) is the set of standard monomials.

Therefore, as a \( k \)-space, \( R/I \) is finite-dimensional. (This is equivalent to saying that ideal \( I \) and the system of polynomials \( G \) are 0-dimensional in the ring-theoretic sense.)

We used this fact in Chapter 1 to construct the multiplication map
\[
M_f : R/I \to R/I, \quad [g] \mapsto [fg]
\]
and applied it to solving the polynomial system \( G \) via eigenvalues of operators \( M_f \) where \( f \) is set equal to one of the variables.

3.3.2. Elimination. Another fundamental problem is that of elimination: given an ideal \( I \subseteq k[x,y] = k[x_1, \ldots, x_n, y_1, \ldots, y_m] \) find \( J = I \cap k[x] \) (an ideal of \( k[x] \)), i.e., eliminate \( y_i \).

Fix a block order \( \gtrsim_{2,1} \) (see §3.2.1) constructed from some monomial orders \( \gtrsim_1 \) on \( k[x] \) and \( \gtrsim_2 \) on \( k[y] \). We say that such order eliminates the variables \( y_i \) and sometimes write \( y_i \gtrsim x_j \) for all \( i, j \).

One can show that if \( G \) is a Gröbner basis of \( I \) with respect to \( \gtrsim_{2,1} \), then \( G \cap k[x] \) is not only a generating set, but also a Gröbner basis of \( J \) with respect to \( \gtrsim_1 \).

Example 3.3.2. Fix the elimination order with \( y \gg x \) on \( R = k[x,y] \) and consider the ideal \( I \) of Example 3.3.1. The set
\[
G = \{x^4 - 2x^3 - x^2 + 2x, 3yx - x^3 - 2x, y^2 - x^2\}
\]
is a Gröbner basis of \( I \) with respect to this order.

Therefore, \( J = I \cap k[x] = \langle x^4 - 2x^3 - x^2 + 2x \rangle \). Now solving the univariate equation and substituting the values of \( x \) in the other equations gives a solving method that was also discussed in Chapter 1.